Guidance on Mitigating Risk Posed by Information Stored on Photocopiers, Fax Machines and Printers

This guidance describes the risk posed by sensitive information stored on certain electronic devices and how institutions should mitigate that risk.

Risk

Photocopiers, fax machines and printers may contain a hard drive or flash memory that stores digital images of the documents that are copied, transmitted or printed by the device. Businesses, public safety agencies and health care providers (organizations) use these devices regularly to process documents which often contain sensitive and confidential information.

Many organizations lease photocopiers, fax machines and printers for a set period of time. At the end of the lease period, the devices are returned to the leasing company and either sold or leased again. Anyone who takes subsequent possession of a device that was used by an organization may be able to access the hard drive or flash memory and view digital images of the documents that were processed by the device, thus giving them access to sensitive personal and business information concerning the organization or its clients.

Controls

Organizations should be aware of the risks posed by the potential disclosure of sensitive information stored on the hard drive or flash memory of photocopiers, fax machines and printers used by the organization. Organizations should implement written policies and procedures to identify devices that store digital images of sensitive documents and ensure their hard drive or flash memory is erased, encrypted or destroyed prior to being returned to the leasing company, sold to a third party or otherwise disposed of. If the organization chooses to erase or encrypt the hard drive, the method used should be sufficiently robust to render the information on the disk unrecoverable. The organizations auditors should ask to review such policies and procedures and verify that they have been effectively implemented.